антных локальных признаков // Радиоэлектроника и информатика. – 2006. – № 1(32). – С. 69–73.
8. *Гонсалес Р., Вудс Р.* Цифровая обработка изображений. – М: Техносфера, 2005. – 1072 с.

Надійшла 27.04.07

Приведені результати досліджень по застосуванню статистичного підходу при формуванні, оцінці значень, аналізі властивостей та установленню еквівалентності характерних ознак зображень в цілях структурного розпізнання об'єктів. Експериментальні оцінки підтверджують можливість побудови оптимальних локальних рішень.

Results of researches on application of the statistical approach are resulted at formation, an estimation of values, the analysis of properties and an establishment of equivalence of characteristic attributes of images with a view of structural recognition of objects. Experimental estimations confirm an opportunity of construction of optimum local decisions.

УДК 681.3.06

В. И. Долгов, А. В. Неласая

ГЕОМЕТРИЧЕСКИЙ ПОДХОД К СЛОЖЕНИЮ ДИВИЗОРОВ ГИПЕРЭЛЛИПТИЧЕСКОЙ КРИВОЙ

В статье приводится понятийный аппарат теории дивизоров гиперэллиптических кривых, а также рассматриваются примеры применения геометрического правила сложения для дивизоров различного типа гиперэллиптической кривой второго рода.

ВВЕДЕНИЕ

Современные мировые стандарты цифровой подписи, в том числе и украинский стандарт ДСТУ 4145–2002, основаны на арифметике эллиптических кривых над конечными полями. Сейчас интерес исследователей направлен еще на одну перспективную алгебраическую структуру – группу дивизоров гиперэллиптических кривых, размер основного поля которых может быть уменьшен в несколько раз в зависимости от рода кривой без потери стойкости. Однако групповая операция в этом случае усложняется.

Целью данной статьи является краткое изложение понятийного аппарата теории дивизоров гиперэллиптических кривых, а также примеров применения геометрического правила сложения различных типов дивизоров кривой второго рода с использованием специализированного математического пакета.

1 ПОНЯТИЙНЫЙ АППАРАТ ТЕОРИИ ДИВИЗОРОВ ГИПЕРЭЛЛИПТИЧЕСКИХ КРИВЫХ

В целях популяризации сведений из теории гиперэллиптических кривых, а также для большего понимания дальнейших рассуждений, следуя работе [1], приведем здесь некоторые важные понятия и определения.

Определение 1. Пусть F – конечное поле и пусть $\overline{F}$ – алгебраическое замыкание F. Гиперэллиптическая кривая C рода $g \geq 1$ над F определяется как множество решений $(x, y) \in F \times F$ уравнения

$$C: y^2 + h(x)y = f(x), \qquad (1)$$

где $h(x) \in F[x]$ – полином степени не более g, $f(x) \in F[x]$ – нормированный полином степени $2g+1$, и при этом не существует решений $(x, y) \in \overline{F} \times \overline{F}$, которые бы одновременно удовлетворяли уравнению (1) и уравнениям с частными производными $2y + h(x) = 0$ и $h'(x)y - f'(x) = 0$.

Для конечной точки $P = (x, y)$ гиперэллиптической кривой C противоположной является точка $-P = (x, -y - h(x))$. Точка на бесконечности P_∞ противоположна сама себе.

Определение 2. Координатным кольцом C над F называется факторкольцо

$$F[C] = F[u, v]/(v^2 + h(u)v - f(u)),$$

где $(v^2 + h(u)v - f(u))$ – идеал в $F[u, v]$, порожденный полиномом $v^2 + h(u)v - f(u)$; $F[u, v]$ – кольцо многочленов от двух переменных, полученное последовательным присоединением к полю F сначала переменной u, а потом v.

Координатное кольцо C над $\overline{F}$ определяется аналогично

$$\overline{F}[C] = \overline{F}[u, v]/(v^2 + h(u)v - f(u)).$$

Говорят, что рациональная функция $R(x, y)$ находится на кривой $C(F)$ если $R(x, y) = 0$ и $C(x, y) = 0$ имеет, по крайней мере, одно решение $P = (X, Y)$, где $X, Y \in F \cup \{\infty\}$, то есть P находится на обоих кривых $R(x, y) = 0$ и $C(x, y) = 0$, что обозначается $P \in R \cap C$.

Элементы $\bar{F}[C]$ рассматриваются как полиномиальные функции, определенные на кривой C.

Определение 3. Поле функций $F(C)$ кривой C над F это поле дробей из элементов $F[C]$. Аналогично, поле функций $\bar{F}(C)$ кривой C над $\bar{F}$ – есть поле дробей из элементов $\bar{F}[C]$. Элементы $\bar{F}(C)$ называются рациональными функциями на C.

Определение 4. Пусть $R \in \bar{F}(C)$ – рациональная функция и пусть $P \in C$, $P \neq \infty$. Тогда R определена в P если существуют полиномиальные функции $G, H \in \bar{F}[C]$, такие что $R = G/H$ и $H(P) \neq 0$; если таких $G, H \in \in \bar{F}[C]$ не существует, то R не определена в P.

Если рациональная функция R определена в точке P, то значением R в P по определению является $R(P) = G(P)/H(P)$. Значение $R(P)$ не зависит от выбора G и H.

Определение 5. Пусть $R \in \bar{F}(C)^*$ и пусть $P \in C$. Тогда, если $R(P) = 0$, то R имеет нуль в точке P. Если R не определена в P тогда R имеет полюс в P, и, следовательно, $R(P) = \infty$.

Справедлива теорема:

Теорема 1. Пусть $P \in C$. Тогда существует функция $U \in \bar{F}(C)$, имеющая в точке P нуль кратности 1 с $U(P) = 0$, для которой выполняется свойство: для каждой полиномиальной функции $G \in \bar{F}[C]^*$ существует целое d и функция $S \in \bar{F}(C)$ такие, что $S(P) \neq 0, \infty$ и $G = U^d S$. Более того, число d не зависит от выбора U. Функция U называется униформизующим параметром для P.

Определение 6. Пусть $G \in \bar{F}[C]^*$ и $P \in C$. Пусть $U \in \bar{F}(C)$ – униформизующий параметр для P, и, следовательно, $G = U^d S$ где $S \in \bar{F}(C)$, $S(P) \neq 0, \infty$. Порядок G в P определяется как $\mathrm{ord}_P(G) = d$.

Из этого определения следует, что порядок функции R в точке P является мерой кратности нулей функции этой функции (см. рис. 1, заимствованный из [2], здесь функция обозначенна f). Другими словами, порядок функции R в точке P есть кратность пересечения кривой C с $R = 0$.

Определение 7. Пусть $R = G/H \in \bar{F}(C)^*$ – рациональная функция на C и $P \in C$. Порядок R в P равен $\mathrm{ord}_P(R) = \mathrm{ord}_P(G) - \mathrm{ord}_P(H)$.

Значение $\mathrm{ord}_p(R)$ является порядком нуля поля функции R на кривой C, а $\mathrm{ord}_p(R^{-1})$ тогда является порядком полюса функции R в точке P.

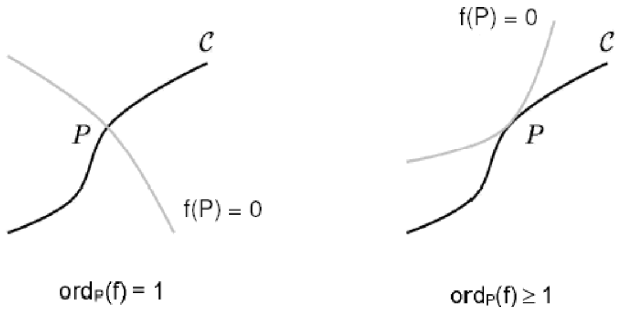

Рисунок 1 – Порядок функции f в точке P

Определение 8. Дивизором на алгебраической кривой называется конечная формальная сумма точек кривой $P_i \in C$

$$D = \sum_{P_i \in C} m_i[P_i], \quad m_i \in Z,$$

где только конечное число m_i не равно нулю.

Степень дивизора D, обозначаемая как $\deg D$, есть целое число, определяемое суммой $\sum_{P \in C} m_p$. Порядок дивизора D в точке P – это целое число m_P: $\mathrm{ord}_p(D) = m_P$. Количество точек дивизора называется весом дивизора.

Множество всех дивизоров формирует аддитивную группу с правилом сложения:

$$\sum_{P_i \in C} m_i[P_i] + \sum_{P_i \in C} n_i[P_i] = \sum_{P_i \in C} (m_i + n_i)[P_i].$$

Символом D^0 обозначается подгруппа, состоящая из дивизоров степени 0.

Ненулевая рациональная функция R, заданная на алгебраической кривой, может иметь лишь конечное число нулей и полюсов. Ее можно задать с точностью до константы списком нулей и полюсов с учетом их кратностей.

Для рациональной функции R на C понятие дивизора определяется следующим образом:

$$\mathrm{div}(R) = \sum_{P \in C} \mathrm{ord}_P(R)[P].$$

Дивизор функции называется главным дивизором. Известно, что $\mathrm{div}(R)$ удовлетворяет условию

$$\sum_{P \in C} \mathrm{ord}_P(R) = 0.$$

Тогда произведению функций на кривой будет соответствовать сумма их дивизоров.

Определение 9. Дивизор $D \in D^0$ называется главным дивизором, если $D = \mathrm{div}(R)$ для некоторых рациональных функций $R \in \bar{F}(C)^*$. Множество всех главных дивизоров обозначим $\mathbb{P}$.

Дивизор $\mathrm{div}(R)$ может быть разложен в разность двух дивизоров:

$$\mathrm{div}(R) = \mathrm{div}_0(R) - \mathrm{div}_\infty(R),$$

где $\mathrm{div}_0(R)$ соответствует пересечению C с кривой $R = 0$, а $\mathrm{div}_\infty(R)$ – пересечению C с функцией $1/R = 0$.

На рис. 2 (здесь обозначение функции f), заимствованным из работы [2], показан пример главного дивизора. Для рассматриваемого примера $\mathrm{div}(R) = P_1 + P_2 + P_3 + P_4 - (2Q_1 + 2Q_2)$.

Функции на гиперэллиптической кривой образуют группу по умножению, поэтому их гомоморфные образы – дивизоры функций образуют группу главных дивизоров и имеют степень 0.

Определение 10. Факторгруппа $J = D^0 / \mathbb{P}$ (группа дивизоров степени 0 по подгруппе главных дивизоров) называется Якобианом кривой C.

Если $D_1, D_2 \in D^0$ и $D_1 - D_2 \in \mathbb{P}$, то D_1 и D_2 называются эквивалентными дивизорами (обозначение $D_1 \sim D_2$). В соответствии с приведенным выше определением, каждый элемент Якобиана – это класс эквивалентности дивизоров.

Определение 11. Дивизор, представленный в виде

$$D = \Sigma_{P \in C} m_i [P_i] - (\Sigma_{P \in C} m_i [P_i])\infty$$

называется приведенным, если:

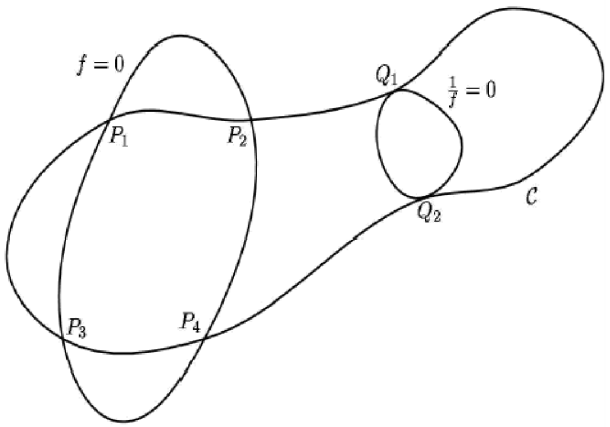

Рисунок 2 – Пример главного дивизора

1. Все m_i неотрицательны, и если $P = -P_i$ тогда $m_i \le 1$.

2. Если $P_i \ne -P_i$, тогда P_i и $-P_i$ встречаются в сумме одновременно.

3. $\sum m_i \le g$.

Каждый смежный класс якобиана обладает ровно одним представителем в виде приведенного дивизора.

Объектами, соответствующими дивизорам, являются идеалы координатного кольца $F[C]$ (см. определение 2) а объектами, соответствующими классам дивизоров, являются классы идеалов $F[C]$. По теореме Римана – Роха главные дивизоры отображаются в главные идеалы. Следовательно, можно рассматривать соответствие между классами дивизоров и классами идеалов. Это позволяет для удобства вычислений использовать интерпретацию дивизоров через классы идеалов полиномиальных порядков. Такое представление в виде пары полиномов было предложено Мамфордом [5].

Лемма 1. Пусть $P = (x, y)$ – обычная точка гиперэллиптической кривой C. Тогда для каждого $k \ge 1$ существует уникальный полином $b_k(u) \in \bar{F}[u]$ такой, что:

1. $\deg_u b_k < k$;

2. $b_k(x) = y$;

3. $b_k^2(u) + b_k(u)h(u) \equiv f(u) (\mathrm{mod}(u - x)^k)$.

Теорема 2. Пусть $D = \sum m_i [P_i] - (\sum m_i)[\infty]$ – приведенный дивизор, где $P_i = (x_i, y_i)$. Пусть $a(u) = \prod (u - x_i)^{m_i}$. Существует уникальный полином $b(u)$, удовлетворяющий:

1. $\deg_u b < \deg_u a$;

2. $b(x_i) = y_i$ для всех i, для которых $m_i \ne 0$;

3. $a(u)$ делит $b(u)^2 + b(u)h(u) - f(u)$.

При выполнении условий теоремы 2

$$D = \gcd(\mathrm{div}(a(u)), \mathrm{div}(b(u) - v)).$$

Обычно запись $\gcd(\mathrm{div}(a(u)), \mathrm{div}(b(u) - v))$ сокращается до $\mathrm{div}(a(u), b(u) - v)$, или, более просто до $\mathrm{div}(a, b)$.

С использованием приведенных понятий и определений рассмотрим особенности выполнения арифметических операций с дивизорами гиперэллиптических кривых.

2 ПРИМЕРЫ ВЫПОЛНЕНИЯ АРИФМЕТИЧЕСКИХ ОПЕРАЦИЙ С ДИВИЗОРАМИ ГИПЕРЭЛЛИПТИЧЕСКИХ КРИВЫХ

Арифметика на гиперэллиптической кривой (операции сложения и дублирования элементов якобиана) реализуется с помощью функций на кривой. Как следует из вышеприведенных рассуждений, якобиан ги-

перэллиптической кривой второго рода включает дивизоры, образованные либо одной, либо двумя точками. Правило сложения хорд и касательных, применимое для эллиптической кривой, в этом случае уже не работает. Исходя из определения якобиана (определение 10), для того, чтобы построить группу, мы должны образовать факторгруппу сумм точек на кривой по подмножеству сумм тех точек, которые лежат на функции, определенной на кривой. В качестве функции на кривой возьмем полином, как обобщение понятия хорды, проходящей более чем через две точки. В общем случае, для нахождения n коэффициентов полинома $y = a_1x^{n-1} + a_2x^{n-2} + \ldots + a_{n-1}x + a_n$ степени $n-1$ достаточно n точек. Сумма всех точек пересечения полученного полинома и заданной эллиптической кривой по определению является дивизором функции и дает нуль рассматриваемой факторгруппы. Пусть $D_1 = P_1 + P_2$ и $D_2 = Q_1 + Q_2$. Необходимо вычислить $D_3 = D_1 + D_2$. Показанная на рис. 3 [2], сумма точек пересечения полученного кубического полинома и гиперэллиптической кривой $P_1 + P_2 + Q_1 + Q_2 + (-R_1) + (-R_2)$ образует нуль группы. На рис. 3, заимствованном из работы [2], показана процедура вычисления суммы точек пересечения кубического полинома и гиперэллиптической кривой $P_1 + P_2 + Q_1 + Q_2 + (-R_1) + (-R_2)$. Эта сумма образует нуль группы. Отсюда очевидно, что противоположной к $(-R_1) + (-R_2)$ суммой $R_1 + R_2$ будет $P_1 + P_2 + Q_1 + Q_2$.

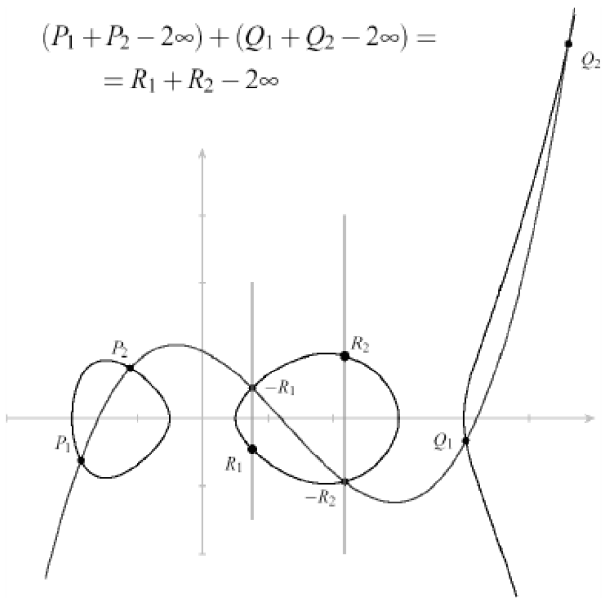

Рисунок 3 – Геометрическая визуализация сложения на кривой второго рода

В зависимости от вида входных дивизоров возможны различные варианты использования описанного правила сложения. В качестве примера рассмотрим гиперэллиптическую кривую

$$y^2 = x^5 + 5x (\mathrm{mod} 73). \qquad (2)$$

Она содержит 49 конечных точек: [27, 4], [53, 1], [53, 72], [36, 23], [36, 50], [56, 28], [56, 45], [37, 36], [37, 37], [32, 54], [32, 19], [21, 41], [9, 57], [12, 20], [12, 53], [9, 16], [41, 2], [41, 71], [61, 29], [64, 67], [64, 6], [29, 22], [29, 51], [72, 33], [44, 10], [44, 63], [27, 69], [46, 35], [46, 38], [72, 40], [50, 68], [24, 14], [61, 44], [24, 59],[21, 32], [49, 60], [49, 13], [50, 5], [0, 0], [1, 15], [1, 58], [17, 26], [17, 47], [52, 12], [52, 61], [20, 27], [20, 46], [23, 11], [23, 62] и бесконечно удаленную точку.

Поскольку данная кривая является кривой Фурукавы, ее порядок можно легко определить по приведенному в [6] алгоритму с помощью программы, разработанной авторами [7]. Полученный порядок, то есть количество приведенных дивизоров якобиана кривой, равен 3842. Все дальнейшие вычисления выполняются в поле $GF(73)$.

Случай 1. Сложение двух дивизоров веса 2. Все точки различны.

P1 = (27, 4),
P2 = (53, 1),
P3 = (56, 45),
P4 = (12, 20).

Представим дивизор D1 = P1 + P2 – 2∞ в форме Мамфорда в виде пары полиномов $<u, v>$.

$$U = (x - 27)(x - 53) = x^2 + 66x + 44.$$

Полином $v = cx + d$ находим из условий

$$\begin{cases} 27*c + d = 4 \\ 53*c + d = 1 \end{cases},$$

откуда имеем $v = 42x + 38$. Следовательно,

$$\mathrm{D1} = \mathrm{P1} + \mathrm{P2} - 2\infty = <x^2 + 66x + 44,\ 42x + 38>.$$

Аналогично

$$\mathrm{D2} = \mathrm{P3} + \mathrm{P4} - 2\infty = <x^2 + 5x + 15,\ 52x + 53>.$$

Для того, чтобы получить дивизор, равный сумме дивизоров D1 и D2 построим кубический полином, проходящий через четыре точки P1, P2, P3, P4 (четыре точки однозначно определяют кубический полином, который имеет четыре коэффициента: коэффициенты

```
> # Все точки различны
restart;
p:=73:
x1:=27:
y1:=4:
x2:=53:
y2:=1:
x3:=56:
y3:=45:
x4:=12:
y4:=20:
S:=msolve ({y1=a1*x1^3+a2*x1^2+a3*x1+a4,
            y2=a1*x2^3+a2*x2^2+a3*x2+a4,
            y3=a1*x3^3+a2*x3^2+a3*x3+a4,
            y4=a1*x4^3+a2*x4^2+a3*x4+a4},p):
a:=subs (S,[a1,a2,a3,a4]):
msolve ({y^2=x^5+5*x,y=a [1]*x^3+a [2]*x^2+a [3]*x+a [4]},p);
        {x = 9, y = 57}, {x = 12, y = 20}, {x = 27, y = 4}, {x = 53, y = 1}, {x = 56, y = 45}, {x = 72, y = 33}
```

при первой, второй и третьей степенях x и свободный член). Для их нахождения необходимо составить четыре уравнения. Это можно сделать, подставив в уравнение кубики поочередно координаты каждой из четырех входных точек. Выполним вычисления с помощью пакета компьютерной алгебры Maple.

Решая совместно систему уравнений, содержащую уравнение кривой и уравнение полученного кубического полинома определим две других точки пересечения (9, 57) и (72, 33). Противоположные к ним точки (9, 16) и (72, 40) и образуют дивизор $<x^2+65x+64,\ 56x+23>$, равный сумме D1 и D2.

Случай 2. Сложение двух дивизоров веса 2. P1 входит в сумму дважды.

P1 = (27, 4),

P2 = (53, 1),

P3 = (32, 19),

$D1 = P1 + P2 - 2\infty = <x^2+66x+44,\ 42x+38>,$

$D2 = P1 + P3 - 2\infty = <x^2+14x+61,\ 3x+69>.$

Если среди четырех исходных точек одна встречается дважды, то подстановкой координат исходных точек в уравнение искомого кубического полинома можно получить только три уравнения. Следовательно, необходимо получить еще одно дополнительное условие, связывающее коэффициенты искомого полинома, для получения четвертого уравнения. Это можно сделать, если учесть тот факт, что в двойной точке полином пересекает заданную гиперэллиптическую кривую дважды, то есть касается ее.

Для кривой, заданной уравнением $f(x, y) = 0$ касательная в точке $P(x_1, y_1)$ имеет вид [3]:

$$\left(\frac{\partial f}{\partial x}\right)\Big|_P (x-x_1)+\left(\frac{\partial f}{\partial y}\right)\Big|_P (y-y_1) = 0.$$

Воспользуемся тем фактом, что в двойной точке касательная к заданной гиперэллиптической кривой совпадет с касательной к искомому полиному. Обозначим $f(x, y): x^5+5x-y^2 = 0$ уравнение заданной гиперэллиптической кривой и $\varphi(x, y): a_1x^3+a_2x^2+a_3x+a_4-y = 0$ уравнение искомого полинома. Тогда

$$\frac{\partial f}{\partial x} = (5x^4+5)\Big|_{(27,\,4)} = 10,$$
$$\frac{\partial f}{\partial y} = (-2y)\Big|_{(27,\,4)} = 65$$

и уравнение касательной к заданной гиперэллиптической кривой в точке (27, 4) имеет вид

$$10(x-27)+65(y-4) = 0. \qquad (3)$$

Аналогично, для искомого кубического полинома

$$\frac{\partial \varphi}{\partial x} = (3a_1x^2+2a_2x+a_3)\Big|_{(27,\,4)} = 3a_1 27^2+2a_2 27+a_3,$$
$$\frac{\partial \varphi}{\partial y} = (-1)\Big|_{(27,\,4)} = -1$$

и уравнение касательной к $\varphi(x, y)$ в точке (27, 4) имеет вид

$$(3a_1 27^2+2a_2 27+a_3)(x-27)-1(y-4) = 0. \qquad (4)$$

```
> # Точка [x1,y1] входит в сумму дважды
p:=73:
x1:=27:
y1:=4:
x2:=53:
y2:=1:
x3:=32:
y3:=19:
f_x:=5*x^4+5:
f_x:=modp1(ConvertIn (f_x,x),p);
f_y:=-2*y:
f_y:=modp1(ConvertIn (f_y,y),p);
f_x_P:=modp1(Eval (f_x,x1),p);
f_y_P:=modp1(Eval (f_y,y1),p);
S:=msolve ({y1=a1*x1^3+a2*x1^2+a3*x1+a4,
            y2=a1*x2^3+a2*x2^2+a3*x2+a4,
            y3=a1*x3^3+a2*x3^2+a3*x3+a4,
            (3*a1*x1^2+2*a2*x1+a3)*(-f_y_P)=f_x_P},p);
a:=subs (S,[a1,a2,a3,a4]);
msolve ({y^2=x^5+5*x,y=a [1]*x^3+a [2]*x^2+a [3]*x+a [4]},p);
            {x = 27, y = 4}, {x = 32, y = 19}, {x = 44, y = 10}, {x = 49, y = 60}, {y = 1, x = 53}
```

Умножим обе части равенства (4) на число (–65), чтобы уравнять коэффициенты при $(y - 4)$ в равенствах (3) и (4). Поскольку два полученных уравнения представляют собой одну и ту же прямую, приравнивая коэффициенты при $(x - 27)$, мы можем записать:

$$(3a_1 27^2 + 2a_2 27 + a_3)(-65) = 10.$$

Это и будет четвертое, недостающее условие, связывающее коэффициенты искомого полинома. Выше приведена реализация в Maple.

Решая совместно систему уравнений, содержащую уравнение кривой и уравнение полученного кубического полинома определим две других точки пересечения (44, 10) и (49, 60). Противоположные к ним точки [44, 63] и [49, 13] образуют дивизор $<x^2 + 53x + 39, 63x + 65>$, равный сумме D1 и D2.

Аналогичный результат можно получить, если входные дивизоры сформированы несколько иным способом:

$D1 = 2P1 - 2\infty = <x^2 + 19x + 72, 56x + 25>$,

$D2 = P2 + P3 - 2\infty = <x^2 + 61x + 17, 20x + 36>$.

В этом случае для представления дивизора D1 в форме Мамфорда воспользуемся уравнением касательной к кривой в точке P1.

$$u = (x - 27)^2 = (x + 46)^2 = x^2 + 19x + 72.$$

В этом случае полином $v = cx + d$ степени ≥ 1 определяется как уравнение касательной к кривой в заданной точке. Пусть кривая C задана уравнением $\varphi(x, y) = 0$. Тогда касательная к C в точке $P(x_1, y_1)$ имеет вид [3]:

$$\left(\frac{\partial\varphi}{\partial x}\right)\Big|_P (x - x_1) + \left(\frac{\partial\varphi}{\partial y}\right)\Big|_P (y - y_1) = 0.$$

Для нашего примера имеем:

$$\varphi(x, y) = x^5 + 5x - y^2,$$

тогда

$$\frac{\partial\varphi}{\partial x} = (5x^4 + 5)\Big|_{(27,\,4)} = 10, \quad \frac{\partial\varphi}{\partial y} = (-2y)\Big|_{(27,\,4)} = 65.$$

Уравнение касательной к кривой в точке (27,4) имеет вид:

$$9(x - 27) + 65(y - 4) = 0;$$
$$y = 56x + 25.$$

Следовательно, $D1 = 2P1 - 2\infty = <x^2 + 19x + 72, 56x + 25>$.

При этом $D2 = P2 + P3 - 2\infty = <x^2 + 61x + 17, 20x + 36>$.

Их сумма также равна $<x^2 + 53x + 39, 63x + 65>$, следовательно, сумма двух дивизоров не зависит от порядка вхождения в них точек кривой.

Рассуждая аналогично, можно получить сумму двух двойных точек или выполнить дублирование, используя условия, определяемые касательными дважды.

```
> # В сумму входят три различных точки
p:=73:
x1:=27:
y1:=4:
x2:=53:
y2:=1:
x3:=32:
y3:=19:
S:=msolve ({y1=a1*x1^2+a2*x1+a3,
            y2=a1*x2^2+a2*x2+a3,
            y3=a1*x3^2+a2*x3+a3},p);
a:=subs (S,[a1,a2,a3]);
msolve ({y^2=x^5+5*x,y=a [1]*x^2+a [2]*x+a [3]},p);
        {y = 15, x = 1}, {x = 27, y = 4}, {x = 29, y = 51}, {y = 19, x = 32}, {x = 53, y = 1}
```

Случай 3. Сумма состоит из трех различных точек, каждая из которых встречается в сумме ровно один раз.

P1 = (27, 4),

P2 = (53, 1),

P3 = (32, 19),

D1 = P1 – ∞ = $<x - 27, 4>$,

D2 = P2 + P3 – 2∞ = $<x^2 + 61x + 17,\ 20x + 36>$.

В этом случае мы строим полином второго порядка $y = a_1x^2 + a_2x + a_3$, требующий наличия трех условий для нахождения трех коэффициентов. Выше приведена реализация в Maple.

Решая совместно систему уравнений, содержащую уравнение кривой и уравнение полученного полинома определим две других точки пересечения (1, 15) и (29, 51). Противоположные к ним точки (1, 58) и (29, 22) и образуют дивизор $<x^2 + 43x + 29,\ 30x + 28>$, равный сумме D1 и D2.

Используя приведенные рассуждения, можно получить решения и для других возможных частных случаев в зависимости от вида входных дивизоров. Если же входные дивизоры содержат противоположные точки, которые аннулируют друг друга, необходимо сначала исключить их из рассмотрения, а затем продолжить сложение оставшихся точек по описанным выше правилам.

ЗАКЛЮЧЕНИЕ

Существует универсальный алгоритм Кантора [4], который можно использовать для сложения дивизоров на гиперэллиптических кривых любого рода. Однако рассмотрение частных случаев, зависящих от вида входных дивизоров, позволяет разработать явные формулы, являющиеся гораздо более быстрыми при программной и аппаратной реализациях. Приведенная в статье иллюстрация геометрического закона сложения дивизоров дает достаточно полное представление о возможных частных случаях, требующих детальной разработки в явном виде.

ПЕРЕЧЕНЬ ССЫЛОК

1. *A. Menezes, Y. Wu, R. Zuccherato.* An Elementary Introduction to Hyperelliptic Curves. – Springer-Verlag, Berlin, Germany, 1998. – 31 p.
2. *T. Wollinger.* Software and Hardware Implementation of Hyperelliptic Curve Cryptosystem. Dissertation for the Degree of Doctor-Ingenieur. – Bochum, Germany, 2004. – 201 p.
3. *Г. Корн, Т. Корн.* Справочник по математике. Для научных работников и инженеров. – М., 1974. – 832 с.
4. *D. G. Cantor.* Computing in Jacobian of a Hyperelliptic Curve // Mathematics of Computation. – Volume 48 (177), January. – 1987. – P. 95–101.
5. *D. Mumford.* Tata Lectures on Theta II // Prog. Math. – Volume 43. – Birkhдuser, 1984. – P. 61–75.
6. *E. Furukava, M. Kawazoe, T. Takahashi.* Counting Points for Hyperelliptic Curves of type $y^2 = x^5 + ax$ over Finite Prime Fields, [Электронный ресурс], (14 p), 2004 – Режим доступа, http://eprint.iacr.org/181.pdf, свободный.
7. *Неласая А. В., Долгов В. И., Зайцев С. А.* Определение порядка группы дивизоров гиперэллиптической кривой // Международная научно-техническая конференция «Компьютерное моделирование и интеллектуальные системы» (КМИС–2007), Запорожье, ЗНТУ, 26–27 марта 2007. – С. 173–177.

Надійшла 11.10.07

У статті приводиться понятійний апарат теорії дивізорів гіпереліптичних кривих, а також розглядаються приклади застосування геометричного правила для додавання дивізорів різного типу гіпереліптичної кривої другого роду.

The conceptual means of divisors hyperelliptic curves theory are considered. The examples of geometrical rule for adding of various kind divisors are given.